Manajemen Resiko Teknologi Informasi Pada Perguruan Tinggi Menggunakan Standar ISO/IEC 27001:2013(Studi Kasus : FTI – UKSW, Salatiga)

Artikel Ilmiah

Peneliti :
Anggrini Kongo
682012057

Program Studi Sistem Informasi
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Salatiga
2016

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan di bawah ini:

Nama	:	Anggrini Kongo		
NIM	:	682012057	Email	: anggrini_kongo@rocketmail.com
Fakultas	:	Teknologi Informasi	Program Studi	: Sistem Informasi
Judul tugas akhir	:	Manajemen Resiko Teknologi Informasi Pada Perguruan Tinggi Menggunakan Standar ISO / IEC 27001 : 2013 (Studi Kasus : FTI – UKSW, Salatiga)		
Pembimbing	:	1. Agustinus Fritz Wijaya, S.Kom, M.Cs		

Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar kesarjanaan baik di Universitas Kristen Satya Wacana maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian/implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan disetujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Kristen Satya Wacana.

Salatiga, 14 September 2016

Anggrini Kongo

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

PERNYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama : Anggrini Kongo

NIM : 682012057 Email : anggrinikongo@rocketmail.com

Fakultas : Teknologi Informasi Program Studi : Sistem Informasi

Judul tugas akhir : Manajemen Resiko Teknologi Informasi Pada Perguruan Tinggi Menggunakan Standar ISO / IEC 27001 : 2013 (Studi Kasus : FTI – UKSW, Salatiga)

Dengan ini saya menyerahkan hak *non-eksklusif** kepada Perpustakaan Universitas – Universitas Kristen Satya Wacana untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tugas akhir elektronik sebagai berikut (beri tanda pada kotak yang sesuai):

☑ a. Saya mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA

☐ b. Saya tidak mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA**

* *Hak yang tidak terbatas hanya bagi satu pihak saja. Pengajar, peneliti, dan mahasiswa yang menyerahkan hak non-ekslusif kepada Repositori Perpustakaan Universitas saat mengumpulkan hasil karya mereka masih memiliki hak copyright atas karya tersebut.*

** *Hanya akan menampilkan halaman judul dan abstrak. Pilihan ini harus dilampiri dengan penjelasan/ alasan tertulis dari pembimbing TA dan diketahui oleh pimpinan fakultas (dekan/kaprodi).*

Demikian pernyataan ini saya buat dengan sebenarnya.

Salatiga, 16 September 2016

Anggrini Kongo

Mengetahui,

Agustinus Fritz Wijaya, S.Kom., M.Cs
Pembimbing I

Manajemen Resiko Teknologi Informasi Pada Perguruan Tinggi
Menggunakan Standar ISO/IEC 27001:2013
(Studi Kasus : FTI – UKSW, Salatiga)

Oleh,

Anggrini Kongo
NIM : 682012057

ARTIKEL ILMIAH

Diajukan Kepada Program Studi Sistem Informasi guna memenuhi sebagian dari persyaratan untuk mencapai gelar Sarjana Sistem Informasi

Disetujui oleh,

Agustinus. Fritz. Wijaya, S. Kom, M. Cs.
Pembimbing 1

Diketahui oleh,

Dr. Dharmaputra T. Palekahelu, M.Pd.
Dekan

Augie David Manuputty, S.Kom., M.Cs.
Ketua Program Studi

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN SATYA WACANA
SALATIGA
2016

Lembar Pengesahan

Judul Tugas Akhir	: Manajemen Resiko Teknologi Informasi Pada Perguruan Tinggi Menggunakan Standar ISO/IEC 27001:2013 (Studi Kasus : FTI – UKSW, Salatiga)
Nama Mahasiswa	: Anggrini Kongo
NIM	: 682012057
Program Studi	: Sistem Informasi
Fakultas	: Teknologi Informasi

Menyetujui,

Agustinus. Fritz. Wijaya, S. Kom, M. Cs.
Pembimbing 1

Mengesahkan,

Dr. Dharmaputra T. Palekahelu, M.Pd.
Dekan

Augie David Manuputty, S.Kom., M.Cs.
Ketua Program Studi

Dinyatakan Lulus tanggal: 9 September 2016

Reviewer :

- Yani Rahardja, S.E., M.M

1. PENDAHULUAN

Dalam era Teknologi Informasi(TI) saat ini , TI telah digunakan sebagai penunjang aktifitas-aktifitas dalam organisasi maupun perusahaan. Dalam dunia pendidikan , TI juga memberikan kemudahan dalam pengolahan data maupun informasi di lembaga sehingga tercapainya suatu kinerja yang efisien dan memberikan pencapaian kualitas layanan yang baik. Dengan perkembangan TI yang sangat pesat, suatu kemungkinan terjadinya gangguan keamanan TI semakin meningkat. Untuk menjamin bahwa segala sesuatunya berjalan seperti yang seharusnya, maka diperlukan manajemen yang baik terhadap setiap layanan IT yang diberikan, seperti melakukan manajemen resiko terhadap TI itu sendiri.

Fakultas Teknologi Informasi(FTI) Univeritas Kristen Satya Wacana(UKSW) adalah sebuah lembaga pendidikan atau perguruan tinggi di Kota Salatiga yang telah menerapkan TI untuk pengelolaan data dan informasi serta layanan di fakultas. Sebagai salah satu fakultas yang memiliki peran penting dalam era teknologi informasi saat ini, FTI-UKSW bersaing ketat dengan lembaga pendidikan/perguruan tinggi lain. Saat ini harapan FTI-UKSW ingin memberikan layanan TI yang baik dan mudah diakses dengan mengintegrasikan semua sistem yang ada dan tentunya jauh dari ancaman. Bagian laboratorium FTI-UKSW adalah divisi yang dipakai untuk menangani setiap kebutuhan TI di fakultas. Salah satu permasalahan TI yang sering dialami oleh FTI-UKSW saat ini adalah website fakultas sering mengalami gangguan secara tiba-tiba sehingga pusat informasi mengalami hambatan yang mengakibatkan mahasiswa sebagai penerima informasi sering mengalami hambatan menerima informasi dari website fakultas tersebut. Di FTI – UKSW untuk melakukan manajemen resiko terhadap ancaman teknologi informasi di fakultas sendiri juga ,belum menggunakan standar internasional khusus untuk melakukan penilaian terhadap resiko yang ada. Perlu diketahui bahwa suatu penilaian resiko sangat penting dilakukan agar setiap resiko tersebut dapat diketahui seberapa besar dampaknya terhadap lembaga / perusahaan. Manfaat dari penilaian resiko sendiri dapat meminimalisir setiap kegagalan dalam sebuah lembaga / perusahaan tersebut. Ada berbagai harapan yang ingin di capai oleh FTI-UKSW, salah satunya yaitu FTI-UKSW ingin memiliki layanan TI yang baik dan mudah diakses dengan mengintegrasikan semua sistem yang ada. Dengan harapan tersebut maka suatu manajemen resiko yang di dalamnya menilai resiko teknologi informasi di FTI – UKSW sangat perlu untuk dilakukan, dengan mengidentifikasi permasalahan maka resiko dan peluang yang ada di FTI – UKSW bisa dapat diketahui dan dilakukan manajemen dengan baik.

Information technology — Security techniques — Information security management systems — Requirements / ISO/IEC 27001: 2013 adalah standar internasional yang telah menyediakan kebutuhan untuk membangun , melaksanakan , menjaga dan terus meningkatkan keamanan informasi dari teknologi informasi untuk sebuah sistem manajemen. ISO/IEC 27001: 2013 memiliki 10 Klausul dan daftar Kontrol yang dapat digunakan untuk dijadikan panduan dalam melakukan manajemen terhadap keamanan

informasi pada teknologi informasi dari organisasi/lembaga/perusahaan. Struktur ISO/IEC 27001: 2013 dapat dijabarkan sebagai berikut ;

1. Scope
2. Normative Reverences
3. Terms and Definitions
4. Context Of The Organisation
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance Evaluation
10. Improvement

Annex A Reference Control Objectives (1)

Berdasarkan informasi diatas, maka melalui penelitian ini dilakukan penilaian resiko TI menggunakan standar ISO/IEC 27001: 2013 dengan memperhatikan Klausul 6 sebagai panduan untuk melakukan penilaian resiko, diharapkan dapat menggunakan hasil dari penilaian ini untuk mengambil kebijakan dalam menangani risiko dan meningkatkan kinerja dalam menjalankan proses bisnis TI di FTI-UKSW.

2. TINJAUAN PUSTAKA

Pada bagian ini dipaparkan mengenai beberapa pengertian terkait penelitian yang dibahas serta sebuah penelitian yang pernah dilakukan peneliti lain terkait topik dan standar yang digunakan.

Resiko

Resiko didefinisikan sebagai peluang terjadinya sesuatu yang dapat memberikan dampak atau mengakibatkan terganggunya proses bisnis organisasi sampai menyebabkan gagalnya tujuan bisnis organisasi. Resiko ini diukur dengan berdasarkan dampak atau pengaruh yang ditimbulkan terhadap kemungkinan terjadinya resiko[2].

Teknologi Informasi

Teknologi informasi atau *Information technology* adalah pengertian umum untuk berbagai jenis teknologi tersedia yang tujuan membantu manusia untuk menjalani hidup dengan lebih mudah dan lebih baik dalam membuat, mengubah, menyimpan, mengkomunikasikan dan atau menyebarkan informasi. Teknologi Informasi menyatukan komputasi dan komunikasi baik dalam berupa data, maupun video yang penerapannya dapat berupa *computer* pribadi, telepon, TV, peralatan rumah elektronik, dan peranti bergerak/mobile(smartphone,computer tablet)[3].

Manajemen Resiko

Manajemen resiko merupakan suatu usaha untuk mengetahui, menganalisis serta mengendalikan resiko dalam setiap kegiatan perusahaan dengan tujuan untuk memperoleh efektifitas dan efisiensi yang lebih tinggi[4].

Manajemen resiko adalah proses untuk mengidentifikasi resiko, menganalisa resiko dan melakukan penanganan untuk mengurangi resiko sampai dampaknya terhadap proses bisnis di organisasi pada level yang dapat diterima atau dibolehkan[2].

Pentingnya Teknologi Informasi dalam Perguruan Tinggi

Pada dasarnya manfaat teknologi informasi dan komunikasi bagi perguruan tinggi dapat dibagi menjadi 2 (dua) kategori besar, kategori pertama disebut sebagai "core values", yaitu terkait dengan manfaat yang diperoleh perguruan tinggi melalui implementasi teknologi informasi dan komunikasi berkaitan langsung dengan proses pembelajaran atau yang di Indonesia berkaitan dengan Tri Dharma perguruan tinggi, dalam konteks ini pemangku kepentingan utama adalah peserta didik(mahasiswa), pendidik (dosen),peneliti, dan pelayan/pengabdi masyarakat. Sementara kategori ke dua disebut sebagai "Supporting values" yaitu terkait dengan manfaat yang diperoleh perguruan tinggi melalui implementasi teknologi informasi dan komunikasi yang berkaitan langsung dengan manajemen penyelengaraan institusi pendidikan tinggi, dalam konteks ini, pemangku kepentingan utamanya adalah pimpinan dan manajemen institusi pendidikan, pemilik(yayasan atau BHP),karyawan, staf, orang tua mahasiswa, mitra kerja, dan pihak terkait lainnya seperti vendor pemasok(supplier), komunitas sekitar,pemerintah/regulator, badan eksternal (seperti BAN, Kopertis), dan lain sebagainya[5].

Manajemen Resiko Teknologi Informasi dengan Standar ISO/IEC 27001:2013

Dalam standar ISO/IEC 27001: 2013 , suatu bentuk pengelolaan resiko teknologi informasi memberikan persyaratan bagaimana suatu organisasi menerapkan teknologi informasi serta melakukan pengelolaan resiko teknologi informasi yang dimiliki oleh organisasi tersebut dengan sebaik mungkin. Standar ISO ISO/IEC 27001: 2013 membantu mempertahankan kerahasiaan, integritas dan ketersediaan informasi terhadap teknologi informasi dengan menerapkan proses manajemen risiko dan memberikan kepercayaan diri kepada pihak yang berkepentingan untuk dikelola risiko secara memadai[1].

Berdasarkan persyaratan standar ISO/IEC 27001 ; 2013, penilaian resiko tidak hanya dilakukan terhadap resiko saja, melainkan juga peluang(resiko positif) yang dimiliki organisasi/lembaga, terkait teknologi informasi yang telah diimplementasikannya. Untuk melakukan manajemen resiko , persyaratan standar ISO/IEC 27001 ; 2013 memberikan persyaratan dengan mengikuti panduan sesuai dengan Klausul 6.1 yaitu terkait Tindakan untuk mengatasi risiko dan peluang[1].

Penelitian Sebelumnya

Penelitian sebelumnya yang terkait dengan penggunaan standar ISO/IEC 27001: 2013 dalam melakukan penilaian resiko pada perguruan tinggi pernah dilakukan oleh Rosmiansi Aprian , dkk., dengan judul "*Perencanaan Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO 27001:2013 (Studi Kasus: Universitas Bina Darma Palembang)"*. Tujuan dari penelitian ini yaitu mengarahkan pada tahap perencanaan SMKI, menentukan kebijakan dan prosedur keamanan informasi pada UBD, dan mengidentifikasi resiko-resiko yang ditemui pada perencanaan SMKI berdasarkan standar ISO 27001:2013. Penelitian ini menghasilkan perancangan dokumen tatakelola keamanan informasi pada teknologi informasi Universitas Bina Darma[6].

3. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian Deskriptif Kualitatif yang bertujuan untuk mengungkapkan suatu masalah atau keadaan tertentu sebagaimana adanya sehingga dapat memberikan gambaran secara tetap tentang keadaan sebenarnya dari objek yang diselidiki dalam rangka memecahkan masalah tertentu yang spesifik[7]. Dalam penelitian ini, wawancara dilakukan terhadap Kepala Bagian Sarana dan Prasarana FTI UKSW sebagai *Key Informan*. *Key informan* atau informan kunci adalah orang atau sekelompok orang yang memiliki informasi Pokok dalam sebuah organisasi atau perusahaan.

Tahapan dalam penelitian ini adalah sebagai berikut ;

1. Studi Literatur
   Mempelajari buku dan jurnal untuk mendapatkan pemahaman lebih tentang topik penelitian
2. Observasi
   Melakukan observasi terhadap objek yang diteliti dan menentukan *Stakeholder* yang akan dilakukan wawancara
3. Wawancara
   Melakukan wawancara dengan *Stakeholder* terkait objek yang diteliti. Pada penelitian ini yaitu Kepala bagian sarana dan prasarana FTI-UKSW.
4. Pengolahan Data
   Melakukan pengolahan data dari hasil wawancara dengan menganalisis data sesuai dengan panduan standar ISO/IEC 27001 ; 2013. Pada Proses analisis resiko dilakukan bersama dengan Kepala Bagian Sarana dan Prasarana FTI-UKSW.

   Tahap dalam pengolahan data digambarkan pada bagan berikut ini ;

Gambar 1. Tahapan Pengolahan Data

5. Laporan
   Melaporkan hasil temuan dan memberikan rekomendasi terhadap lembaga.

4. HASIL DAN PEMBAHASAN

Berdasarkan hasil wawancara dengan *key informan* didapatkan beberapa resiko dan peluang teknologi informasi yang dimiliki oleh FTI UKSW yang dapat disajikan dalam Tabel 1 berikut ini ;

Table 1. Identifikasi Resiko dan Peluang yang ada di FTI -UKSW

Jenis	Resiko	Penyebab
Resiko	Dikenakan Regulasi DMCA	Beberapa software belum berlisensi karena kurang ada dukungan dana software berlisensi
Resiko	Beberapa sistem informasi sulit di akses	Web hosting masih dipegang pihak luar dan sering mengalami down
Peluang	Sejauh ini FTI memiliki Infrastuktur IT yang memenuhi spesifikasi	Ketika ada permintaan , FTI memiliki cukup dana untuk memenuhi semua permintaan sesuai dengan hasil rapat kerja

Resiko	Kerusakan infrastruktur	Listrik mati dan bencana alam yang dapat merusak beberapa infrasktruktur
Resiko	Mematikan server secara sengaja	Lokasi server yang diketahui banyak orang, masih terpisah-pisah karena keterbatasan ruangan
Peluang	Memindahkan server ke BTSI UKSW	Adanya hubungan kerja sama dengan BTSI UKSW , BTSI UKSW bisa menangani keterbatasan server di FTI
Resiko	Kurangnya kemampuan sumber daya dalam laboran FTI	Skill yang dirasakan masih kurang dalam kinerja di laboran
Resiko	Terhambatnya akses data karena masalah jaringan komputer yang belum segera tertangani oleh SDM	Misskomunikasi yang masih sering terjadi antar sumber daya manusia(karwayan di laboran FTI)

FTI – UKSW memiliki 6 Resiko Teknologi Informasi dan 2 Peluang Teknologi Informasi. Dari hasil di atas selanjutnya akan dipakai untuk dilakukannya penilaian resiko dan peluang tersebut, dengan melakukan lagi penilaian terhadap Resiko Melekat(Inherent Risk) dengan tujuan mengetahui sejauh mana dampak resiko dan peluang tersebut bisa terjadi di setiap keadaan di FTI-UKSW.

Identifikasi Resiko dan Resiko melekat (Inherent Risk)

Berdasarkan panduan standar ISO / IEC 27001: 2013, resiko dan peluang harus dibuat kriteria resiko yang dapat dipetakan ke dalam kategori, jenis,penyebab dan konsekuensi.

Setelah diketahui beberapa resiko dan peluang yang dimiliki oleh Laboratorium FTI-UKSW terkait masalah teknologi informasi, pada Tabel 2 dibawah ini dijabarkan proses kriteria tersebut. Tujuannya agar resiko dan peluang tersebut dapat lebih jelas diidentifikasi, dan juga dapat dinilai besar resiko atau peluang tersebut dengan dilakukannya proses analisis resiko melekat(inherent risk) yang meliputi kemungkinan terjadinya resiko, konsekuensi terjadinya resiko, tingkat resiko dan selanjutnya akan mengambil *control* untuk menangani resiko atau peluang tersebut berdasarkan *Annex A Reference Control Objectives* ISO / IEC 27001: 2013.

Table 2. Identifikasi Resiko dan Resiko melekat (Inherent Risk)

Identifikasi Resiko					**Resiko melekat (Inherent Risk)**		
Kategori	**Jenis**	**Resiko**	**Pennyebab**	**Konsekuensi**	**Kemungkinan**	**Konsekuensi**	**Tingkat Resiko**

Software	Resiko	Dikenakan Regulasi DMCA	Software belum berlisensi karena kurang ada dukungan dana software berlisensi	Pelanggaran perundang-undangan yang dapat dikenakan pasal	Likely	Major	Extreme Risk
Software	Resiko	Beberapa sistem informasi sulit di akses	Web hosting masih dipegang pihak luar dan sering mengalami down	Tersendatnya layanan, dan masih sulit ditangani secara langsung karena masih ditangani pihak luar	Almost certain	Catastropic	Extreme Risk
Infrastructure	Peluang	Sejauh ini FTI memiliki Infrastuktur IT yang memenuhi spesifikasi	Ketika ada permintaan , FTI memiliki cukup dana untuk memenuhi semua permintaan sesuai dengan hasil rapat kerja	Meningkatnya perfoma layanan	Almost certain	Catastropic	Extreme Risk
Infrastructure	Resiko	Kerusakan infrastruktur	Listrik mati dan bencana alam yang dapat merusak beberapa infrasktruktur	Tersendatnya layanan,	Likely	Catastropic	Extreme Risk
Hardware Security	Resiko	Mematikan server secara sengaja	Lokasi server yang diketahui banyak orang, masih terpisah-pisah karena keterbatasan ruangan	Tersendatnya layanan dan transaksi data(jika ada transaksi)	Moderate	Moderate	High Risk
Harware Security	Peluang	Memindahkan server ke BTSI UKSW	Adanya hubungan kerja sama dengan BTSI UKSW , BTSI UKSW bisa menangani keterbatasan server di FTI	Meningkatkan performa layanan	Almost certain	Catastropic	Extreme Risk
Human resource	Resiko	Kurangnya kemampuan sumber daya dalam laboran FTI	Skill yang dirasakan masih kurang dalam kinerja di laboran	Pemanfaatan TI untuk meningkatkan performa belum sepenuhnya terpenuhi	Almost certain	Major	Extreme Risk

Human resource	Resiko	Terhambatnya akses data karena masalah jaringan komputer yang belum segera tertangani oleh SDM	Misskomunikasi yang masih sering terjadi antar sumber daya manusia(karwayan di laboran FTI	Terhambatnya akses data dan informasi	Moderate	Moderate	High Risk

Resiko melekat (Inherent Risk)

Pada Tabel 2 di atas penilaian Resiko Melekat atau *inherent risk* dilakukan agar dapat diketahui sejauh mana suatu resiko dan peluang di FTI-UKSW dapat saja menjadi suatu dampak *negative* ataupun *positive* bagi pelayanan di fakultas .

Dari hasil yang didapatkan melalui wawancara dan penilaian langsung bersama *Key Informan* berdasarkan pengalaman permasalahan yang terjadi terkait teknologi informasi di FTI - UKSW, telah dijabarkan di atas juga hasil Kemungkinan dan Konsekuesi sesuai Penilaian Kemungkinan (Likelihood) pada Tabel 3 dan Penilaian Konsekuensi (Consequences) pada Tabel 5 di bawah ini ;

Table 3. Penilaian Kemungkinan(Likelihood)(8)

Likelihood Qualitative Measure	**Description**
Almost Certain	The event is expected to occur in most circumstances (one or more times per year).
Likely	The event will probably occur in most circumstances (once in two years).
Moderate	The event should occur at some time (once in five years).
Unlikely	The event could occur at some time (once in ten years).
Rare	The event may occur only in exceptional circumstances (once in fifty years).

Menilai Kemungkinan itu penting untuk menentukan jangka waktu sebuah resiko atau peluang tersebut dapat saja terjadi, dengan melihat kembali penyebab – penyebab resiko dan peluang teknologi informasi. Contoh dari hasil penilaian Kemungkinan, Misalnya kemungkinan suatu peristiwa tersebut dapat terjadi dalam waktu 5 tahun.

Dari penilaian Tabel 3 di atas, hasil Penilaian Kemungkinan berdasarkan resiko dan peluang di FTI – UKSW adalah sebagai berikut ;

Table 4. Hasil Penilaian Kemungkinan(Likelihood)

Identifikasi Resiko					**Resiko melekat (Inherent Risk)**
Kategori	**Jenis**	**Resiko**	**Pennyebab**	**Konsekuensi**	**Kemungkinan (Likelihood)**

Software	Resiko	Dikenakan Regulasi DMCA	Software belum berlisensi karena kurang ada dukungan dana software berlisensi	Pelanggaran perundang-undangan yang dapat dikenakan pasal	Likely
Software	Resiko	Beberapa sistem informasi sulit di akses	Web hosting masih dipegang pihak luar dan sering mengalami down	Tersendatnya layanan, dan masih sulit ditangani secara langsung karena masih ditangani pihak luar	Almost certain
Infrastructure	Peluang	Sejauh ini FTI memiliki Infrastuktur IT yang memenuhi spesifikasi	Ketika ada permintaan , FTI memiliki cukup dana untuk memenuhi semua permintaan sesuai dengan hasil rapat kerja	Meningkatnya perfoma layanan	Almost certain
Infrastructure	Resiko	Kerusakan infrastruktur	Listrik mati dan bencana alam yang dapat merusak beberapa infrasktruktur	Tersendatnya layanan,	Likely
Hardware Security	Resiko	Mematikan server secara sengaja	Lokasi server yang diketahui banyak orang, masih terpisah-pisah karena keterbatasan ruangan	Tersendatnya layanan dan transaksi data(jika ada transaksi)	Moderate
Harware Security	Peluang	Memindahkan server ke BTSI UKSW	Adanya hubungan kerja sama dengan BTSI UKSW , BTSI UKSW bisa menangani keterbatasan server di FTI	Meningkatkan performa layanan	Almost certain
Human resource	Resiko	Kurangnya kemampuan sumber daya dalam laboran FTI	Skill yang dirasakan masih kurang dalam kinerja di laboran	Pemanfaatan TI untuk meningkatkan performa belum sepenuhnya terpenuhi	Almost certain

Human resource	Resiko	Terhambatnya akses data karena masalah jaringan komputer yang belum segera tertangani oleh SDM	Misskomunikasi yang masih sering terjadi antar sumber daya manusia(karyawan di laboran FTI	Terhambatnya akses data dan informasi	Moderate

Setelah dilakukan Penilaian Kemungkinan (Likelihood) , Selanjutnya dilakukan penilaian Konsekuensi (Consequences). Penilaian Konsekuensi (Consequences) berbeda dengan penilaian kemungkinan, namun keduanya memiliki hubungan dimana penilaian kemungkinan bisa mempengaruhi penilaian konsekuensi yang ditimbulkan dari resiko dan peluang yang ada. Pada Tabel 5 di bawah ini merupakan tingkat penilaian konsekuensi beserta penjelasannya.

Tabel 5. Penilaian Konsekuensi(Consequences)(8)

Consequences **Qualitative Measure**	**Description**
Catastrophic	The consequences would threaten the provision of key services, causing major problems for customers, the Government and the agency. Possible loss of greater than $10 million.
Major	The consequences would threaten the continued effective provision of services and require top level management or Ministerial intervention. Possible loss of between $5 million and $10 million.
Moderate	The consequences would not threaten the provision of services, but would mean the agency would be subject to review or changed ways of functioning. Possible loss of between $1 million and $5 million.
Minor	The consequences would threaten the efficiency or effectiveness of some services, but could be dealt with internally. Possible loss of between $100,000 and $1 million.

Insignificant	The consequences are dealt with by routine operations. Possible loss of less than $100,000.

Dari hasil penilaian menggunakan Tabel Penilaian Konsekuensi di atas, didapatkan hasil Penilaian Konsekuensi (Consequences**)** dari resiko dan peluang yang dimiliki FTI –UKSW dapat dilihat pada Tabel 6 di bawah ini ;

Tabel 6. Hasil Penilaian Konsekuensi(Consequences)

Identifikasi Resiko					**Resiko melekat (Inherent Risk)**	
Kategori	**Jenis**	**Resiko**	**Pennyebab**	**Konsekuensi**	**Kemungkinan (Likelihood)**	**Konsekuensi (Consequences)**
Software	Resiko	Dikenakan Regulasi DMCA	Software belum berlisensi karena kurang ada dukungan dana software berlisensi	Pelanggaran perundang-undangan yang dapat dikenakan pasal	Likely	Major
Software	Resiko	Beberapa sistem informasi sulit di akses	Web hosting masih dipegang pihak luar dan sering mengalami down	Tersendatnya layanan, dan masih sulit ditangani secara langsung karena masih ditangani pihak luar	Almost certain	Catastropic
Infrastructure	Peluang	Sejauh ini FTI memiliki Infrastuktur IT yang memenuhi spesifikasi	Ketika ada permintaan , FTI memiliki cukup dana untuk memenuhi semua permintaan sesuai dengan hasil rapat kerja	Meningkatnya perfoma layanan	Almost certain	Catastropic
Infrastructure	Resiko	Kerusakan infrastruktur	Listrik mati dan bencana alam yang dapat merusak beberapa infrasktruktur	Tersendatnya layanan,	Likely	Catastropic
Hardware Security	Resiko	Mematikan server secara sengaja	Lokasi server yang diketahui banyak orang, masih terpisah-pisah karena keterbatasan ruangan	Tersendatnya layanan dan transaksi data(jika ada transaksi)	Moderate	Moderate

Harware Security	Peluang	Memindahkan server ke BTSI UKSW	Adanya hubungan kerja sama dengan BTSI UKSW , BTSI UKSW bisa menangani keterbatasan server di FTI	Meningkatkan performa layanan	Almost certain	Catastropic
Human resource	Resiko	Kurangnya kemampuan sumber daya dalam laboran FTI	Skill yang dirasakan masih kurang dalam kinerja di laboran	Pemanfaatan TI untuk meningkatkan performa belum sepenuhnya terpenuhi	Almost certain	Major
Human resource	Resiko	Terhambatnya akses data karena masalah jaringan komputer yang belum segera tertangani oleh SDM	Misskomunikasi yang masih sering terjadi antar sumber daya manusia(karwayan di laboran FTI	Terhambatnya akses data dan informasi	Moderate	Moderate

Dari hasil Penilaian Kemungkinan (Likelihood) dan Konsekuensi (Consequences) ,dapat disimpulkan bahwa besar kemungkinan suatu resiko dapat terjadi dalam beberapa kali dalam kurung 2 tahun sampai 5 tahun. Sedangkan peluang (resiko positif) memberikan hasil yang cukup baik dimana peluang tersebut bisa terjadi beberapa kali dalam setahun.

Sedangkan untuk hasil Konsekuensi dari resiko dan peluang tersebut bahwa FTI – UKSW memiliki ancaman resiko teknologi informasi yang cukup tinggi , dimana beberapa penyebab resiko dan peluang memberikan konsekuensi yang dapat mengancam penyedia layanan ,menyebabkan masalah besar, dan kerugian bagi layanan maupun civitas yang ada di FTI – UKSW. Bahkan dengan melihat kondisi tersebut, menurut hasil analisis dan wawancara beberapa permasalahan juga masih dapat ditangani oleh laboratorium FTI – UKSW , namun tidak menutup kemungkinan nantinya laboratorium FTI – UKSW juga akan segera melakukan penanganan lebih lanjut.

Penilaian Tingkat Resiko

Tahapan selanjutnya yaitu menilai Tingkat Resiko. Terdapat 4 level Tingkat Resiko dimulai dari level terendah hingga tertinggi (Low Risk, Moderate Risk, High Risk, Extreme Risk) yang dapat digunakan sebagai pengukuran tingkat resiko dan peluang yang dimiliki FTI – UKSW agar resiko dan peluang tersebut menjadi perhatian penting bagi manajemen. Penilaian tingkat resiko juga dapat membantu menentukan Pemilik Resiko yang bertanggung jawab untuk selalu mengawasi dan mengevaluasi resiko dan peluang tersebut. Untuk melakukan Penilaian Tingkat Resiko harus dilakukan dengan

Risk Matrix pada Tabel 7 di bawah dengan memperhatikan hasil dari Penilaian Kemungkinan (Likelihood) dan Konsekuensi (Consequences).

Penilaian Tingkat Resiko (8)
E = Extreme Risk – Immediate Action Required
H = High Risk – Senior Management Attention Required
M = Moderate Risk – Management Responsibility must be Specified
L = Low Risk – Manage by Routine Procedures

Tabel 7. Risk Matrix(3)

Likelihood	**Consequence**				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	H	H	E	E	E
Likely	M	H	H	E	E
Moderate	L	M	H	E	E
Unlikely	L	L	M	H	E
Rare	L	L	M	H	H

Dari hasil penilaian tingkat resiko secara keseluruhannya dapat dilihat pada Tabel 8 di bawah ini , dengan memperhatikan hasil Tingkat Resiko pada Penilaian Resiko Melekat (Inherent Risk).

Tabel 8. Hasil Keseluruhan Penilaian

Identifikasi Resiko					**Resiko melekat (Inherent Risk)**		
Kategori	**Jenis**	**Resiko**	**Pennyebab**	**Konsekuensi**	**Kemungkinan**	**Konsekuensi**	**Tingkat Resiko**
Software	Resiko	Dikenakan Regulasi DMCA	Software belum berlisensi karena kurang ada dukungan dana software berlisensi	Pelanggaran perundang-undangan yang dapat dikenakan pasal	Likely	Major	Extreme Risk
Software	Resiko	Beberapa sistem informasi sulit di akses	Web hosting masih dipegang pihak luar dan sering mengalami down	Tersendatnya layanan, dan masih sulit ditangani secara langsung karena masih ditangani pihak luar	Almost certain	Catastropic	Extreme Risk

Infrastructure	Peluang	Sejauh ini FTI memiliki Infrastuktur IT yang memenuhi spesifikasi	Ketika ada permintaan , FTI memiliki cukup dana untuk memenuhi semua permintaan sesuai dengan hasil rapat kerja	Meningkatnya perfoma layanan	Almost certain	Catastropic	Extreme Risk
Infrastructure	Resiko	Kerusakan infrastruktur	Listrik mati dan bencana alam yang dapat merusak beberapa infrasktruktur	Tersendatnya layanan,	Likely	Catastropic	Extreme Risk
Hardware Security	Resiko	Mematikan server secara sengaja	Lokasi server yang diketahui banyak orang, masih terpisah-pisah karena keterbatasan ruangan	Tersendatnya layanan dan transaksi data(jika ada transaksi)	Moderate	Moderate	High Risk
Harware Security	Peluang	Memindahkan server ke BTSI UKSW	Adanya hubungan kerja sama dengan BTSI UKSW , BTSI UKSW bisa menangani keterbatasan server di FTI	Meningkatkan performa layanan	Almost certain	Catastropic	Extreme Risk
Human resource	Resiko	Kurangnya kemampuan sumber daya dalam laboran FTI	Skill yang dirasakan masih kurang dalam kinerja di laboran	Pemanfaatan TI untuk meningkatkan performa belum sepenuhnya terpenuhi	Almost certain	Major	Extreme Risk
Human resource	Resiko	Terhambatnya akses data karena masalah jaringan komputer yang belum segera tertangani oleh SDM	Misskomunikasi yang masih sering terjadi antar sumber daya manusia(karwayan di laboran FTI	Terhambatnya akses data dan informasi	Moderate	Moderate	High Risk

Hasil menunjukan bahwa resiko dan peluang di FTI - UKSW masuk pada *Extreme Risk* dan *High Risk*.

Evaluasi Resiko

Standar ISO/IEC 27001 ; 2013 juga memberikan panduan dalam mengevaluasi resiko maupun peluang yang telah diidentifikasi dan dianalisis.

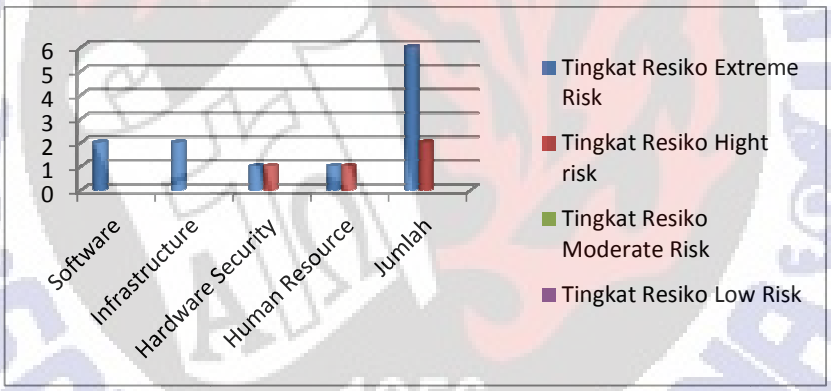
Dalam mengevaluasi, dilakukan dengan membandingkan hasil analisis resiko dengan kriteria resiko yang telah dibangun dan memprioritaskan dianalisisnya resiko tersebut untuk penanganan resiko.

Pada penelitian ini, proses mengevaluasi resiko dan peluang dilakukan dengan membandingkan hasil analisis resiko (Penilaian Kemungkinan (Likelihood), Penilaian Konsekuensi (Consequences) , Tingkat Resiko) dengan Kriteria Resiko (Kategori , Jenis, Resiko, Penyebab,Konsekuensi).

Pada proses dan hasil dari evaluasi resiko, dapat digambarkan dalam Diagram yang dapat dilihat pada Gambar 2 di bawah ini terkait Tingkat dan Jumlah Resiko.

Diagram Tingkat dan Jumlah Resiko

Diagram pada Gambar 2 di bawah ini digambarkan sesuai dengan tingkat resiko dari kategori resiko dan peluang yang dapat dilihat dari Tabel 8. Dari diagram tersebut, dapat ditarik kesimpulan bahwa tingkat resiko *Extreme risk* sangat tinggi dengan jumlah resiko di dalamnya juga peluang yaitu 6, sedangkan *Hight risk* terdapat 2 resiko/peluang. Semua Kategori masuk pada *Extreme risk* sedangkan 1 dari *Hardware security* dan *Human resource* masuk dalam *Hight risk*. Dengan demikian, FTI – UKSW memiliki resiko dan peluang teknologi informasi yang tinggi terhadap dampak negative yang dapat ditimbulkan yang mengakibatkan kerugian ataupun kegagalan pada layanan teknologi informasi yang telah diimplementasikan.



Gambar 2. Tingkat dan Jumlah Resiko

5. SIMPULAN DAN SARAN

Dalam simpulan dan saran dijabarkan beberapa rekomendasi untuk Resiko dan Peluang di FTI-UKSW berdasarkan control standar ISO/IEC 27001; 2013.

Simpulan

Berdasarkan hasil analisis di atas, maka dapat disimpulkan bahwa Resiko dan peluang TI di FTI-UKSW sangat diperlukan untuk segera dilakukan penanganan untuk lebih baik lagi. Maka dari hasil penelitian ini, dapat diberikan rekomendasi untuk

melakukan manajemen resiko sesuai dengan Control ISO/IEC 27001; 2013 dari hasil identifikasi dan analisis resiko dan peluang yang ada di FTI-UKSW. Dari hasil analisis resiko diatas juga telah memberikan hasil pengukuran tingkat resiko guna untuk menentukan pemilik resiko yang ditambahkan dalam rekomendasi di bawah ini. Tugas dari pemilik resiko yaitu memantau atau mengawasi setiap resiko dan peluang yang dimiliki oleh FTI UKSW . Hasil rekomendasi tersebut adalah sebagai berikut ini;

1. **Software** : Resiko dikenakan Regulasi DMCA karena beberapa software yang digunakan belum berlisensi.
   Control :
   - Sebaiknya segera dilakukan negosiasi dengan bagian keuangan untuk mendapatkan dana pembelian software berlisensi.

   Pemilik Resiko : Senior manajemen
2. **Software** : Beberapa sistem informasi sulit diakses karena web hosting masih dipegang pihak luar.
   Control :
   - Perjanjian dengan pihak luar meliputi persyaratan untuk mengatasi risiko keamanan informasi yang terkait dengan informasi dan layanan teknologi komunikasi

   Pemilik Resiko: Senior manajemen
3. **Infrastructure** : Sebuah peluang , sejauh ini FTI memiliki Infrastuktur IT yang memenuhi spesifikasi.
   Control :
   - Memastikan bahwa penggunaan teknologi informasi di FTI berjalan dengan optimal dan sesuai dengan kebutuhan

   Pemilik Resiko : Senior manajemen
4. **Infrastructure** : Resiko kerusakan infrastruktur karena bencana alam dan listrik mati
   Control :
   - Perlindungan fisik terhadap bencana alam, serangan berbahaya atau kecelakaan harus dirancang dan diterapkan.
   - Kepuasan penggunaan program yang mungkin mampu override sistem dan aplikasi harus dibatasi dan dikontrol erat
   - Setiap sistem informasi ataupun layanan wajib dicatat dan melaporkan setiap kelemahan keamanan informasi yang diamati atau dicurigai.

   Pemilik Resiko : Senir manajemen
5. **Hardware security** : Resiko mematikan server secara sengaja karena Lokasi server yang diketahui banyak orang, masih terpisah-pisah karena keterbatasan ruangan.
   Control :
   - Perimeter/kawasan keamanan harus ditetapkan dan digunakan untuk melindungi daerah daerah yang berisi baik informasi dan fasilitas pengolahan informasi yang sensitif atau kritis.
   - Keamanan fisik untuk kantor dan fasilitas harus dirancang dan diterapkan.

- Memastikan hanya karyawan yang berwenang yang dapat mengakses lokasi server.

Pemilik Resiko : Senior manajemen

6. **Harware security**: Sebuah peluang bahwa FTI dapat memindahkan server ke BTSI UKSW

   Control :

   - Semua persyaratan keamanan informasi yang relevan harus ditetapkan dan disetujui dengan pihak BTSI yang dapat mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur TI untuk informasi di FTI

   Pemilik Resiko : Senior manajemen

7. **Human resource** : Kurangnya kemampuan sumber daya manusia dalam laboran FTI, karena kemampuan yang dirasakan masih kurang dalam kinerja di laboran

   Control :

   - Melakukan pelatihan terhadap SDM sehingga memiliki standar penggunaan TI

   Pemilik Resiko : Senior manajemen

8. **Human resource** : Terhambatnya akses data karena masalah jaringan komputer yang belum segera tertangani oleh SDM karena masalah misskomunikasi antar SDM yang masih sering terjadi

   Control :

   - Tanggung jawab manajemen dan prosedur harus ditetapkan untuk memastikan respon yang cepat, efektif dan teratur untuk insiden keamanan informasi
   - Harus ada suatu proses disipliner formal yang harus dikomunikasikan laboran FTI untuk mengambil tindakan terhadap SDM yang telah melakukan suatu pelanggaran keamanan informasi.

   Pemilik Resiko : Senior manajemen

Saran

Adapun beberapa saran yang dapat peneliti berikan terkait manajemen resiko dan peluang TI untuk FTI-UKSW diantaranya (1) Perlu adanya prosedure penangangan resiko terkait TI yang digunakan, (2) Perlu adanya persyaratan/kontrak yang jelas dengan pihak luar mengenai resiko yang masih sering terjadi dibawa pihak luar, (3) Kepala Sarana dan Prasarana dalam hal ini Kepala bagian Laboratorium FTI-UKSW sebagai senior manajemen segera mengkomunikasikan permasalahan TI yang masih dan kemungkinan akan terjadi di FTI-UKSW dengan pimpinan fakultas dan manajemen untuk segera dilakukan penanganan, agar tercapainya harapan FTI – UKSW dimana ingin memiliki layanan TI yang baik dan mudah diakses.

6. DAFTAR PUSTAKA

[1]. ISO(International Organization for Standardization).,2013., *International Standard ISO/IEC 27001*. Ed.2. Switzerland :ISO.

[2]. Sarno,R. & Iffano,I., 2009.,*Sistem Manajemen Keamanan Informasi*. Surabaya: ITSPress.

[3]. Irwansyah,E & Moniaga.V.J.,2014., *Pengantar Teknologi Informasi*.ed.1.Yogyakarta: deepublish

[4]. Darmawi, H., 1999., *Manajement Resiko*. Jakarta : Bumi Aksara.

[5]. Indrajit,E.R.,2011.,Peran *Teknologi Informasi pada perguruan Tinggi*. Indonesia: Aptikom

[6]. Aprian,R,Rizal,S & Sobri.M.,2015., Perencanaan Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO 27001:2013*, Jurnal Informatika Universitas Bina Darma Palembang, digilib.binadarma.ac.id*

[7]. Kimbal,W,R.,2015.,*Modal Sosial dan Ekonomi Industry Kecil Sebuah Studi Kualitatif*.ed.1.Yogyakarta: deepublish

[8]. Department Of Commerce.,2003.,*Information Security Guideline for NSW Government – Part 1 Information Security Risk Management* Ed.2.